AMENDMENTS TO THE CLAIMS

1. (PREVIOUSLY PRESENTED) A method in a router having at least one outbound interface, the method comprising:

establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module, each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number;

controlling supply of data packets to the cryptographic module by:

(1) assigning, for each secure connection, a corresponding queuing module,

(2) reordering, in each queuing module, a corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and

(3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets; and

second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated secure connections.

2. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

3. (ORIGINAL) The method of claim 1, wherein the reordering step includes, in each queuing module:

establishing a plurality of queues having respective identified priorities;

storing each data packet associated with the corresponding secure connection in one of

the queues based on a corresponding identified priority for said each data packet; and

selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy.

4. (ORIGINAL) The method of claim 1, wherein:

the establishing step includes establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module;

the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections;

the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router.

5. (ORIGINAL) The method of claim 1, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

6. (ORIGINAL) The method of claim 5, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream and an audio stream.

7. (ORIGINAL) The method of claim 6, wherein the audio stream is a Voice over IP media stream.

8. (ORIGINAL) The method of claim 1, wherein the controlling step further includes obtaining, for each queuing module, the corresponding assigned maximum output bandwidth from a configuration register.

9. (ORIGINAL) The method of claim 1, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination.

10. (ORIGINAL) A router comprising:

a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers;

an outbound interface configured for establishing a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving respective streams of the encrypted packets; and

a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module, each queuing module configured for:

(1) outputting to the cryptographic module a corresponding group of the data packets associated with the corresponding secure connection, and according to a corresponding assigned maximum output bandwidth for the corresponding queuing module, for generation of the corresponding stream of the encrypted packets, and

(2) reordering the corresponding group of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth.

11. (ORIGINAL) The router of claim 10, wherein each queuing module is configured for reordering the corresponding group of the data packets in response to detection of a congestion condition in the outbound interface having established the corresponding secure connection.

12. (ORIGINAL) The router of claim 10, wherein each queuing module is configured for:

establishing a plurality of queues having respective identified priorities;

storing each data packet associated with the corresponding secure connection in one of

the queues based on a corresponding identified priority for said each data packet; and

selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy.

13. (ORIGINAL) The router of claim 10, wherein the cryptographic module is configured for outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

14. (ORIGINAL) The router of claim 13, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream and an audio stream.

15. (ORIGINAL) The router of claim 14, wherein the audio stream is a Voice over IP media stream.

16. (ORIGINAL) The router of claim 10, wherein the queue controller includes a configuration register configured for storing, for each queuing module, the corresponding assigned maximum output bandwidth.

17. (ORIGINAL) The router of claim 10, wherein the queue controller includes a peer bandwidth module configured for negotiating, for each queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination.

18. (PREVIOUSLY PRESENTED) A computer readable medium having stored thereon sequences of instructions for outputting encrypted packets by a router having at least one outbound interface, the sequences of instructions including instructions for:

establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module, each encrypted packet successively output from the cryptographic module

having a corresponding successively-unique sequence number;

controlling supply of data packets to the cryptographic module by:

(1) assigning, for each secure connection, a corresponding queuing module,

(2) reordering, in each queuing module, a corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and

(3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets; and

second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated secure connections.

19. (PREVIOUSLY PRESENTED) The medium of claim 18, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

20. (ORIGINAL) The medium of claim 18, wherein the reordering step includes, in each queuing module:

establishing a plurality of queues having respective identified priorities;

storing each data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each data packet; and

selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy.

21. (ORIGINAL) The medium of claim 18, wherein:

the establishing step includes establishing, on each of a plurality of the outbound

interfaces, a corresponding plurality of the secure connections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module;

the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections;

the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router.

22. (ORIGINAL) The medium of claim 18, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

23. (CANCELED).

24. (CANCELED).

25. (CANCELED).

26. (ORIGINAL) The medium of claim 18, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination.

27. (ORIGINAL) A router having at least one outbound interface, the router further comprising:

means for establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets;

means for generating the encrypted packets, each encrypted packet successively output

having a corresponding successively-unique sequence number; and

means for controlling supply of data packets to the generating means, including:

(1) means for assigning, for each secure connection, a corresponding queuing means for queuing data packets,

(2) means for reordering, in each queuing means, a corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing means, the means for reordering configured for outputting to the generating means the group of data packets, from each corresponding queuing means according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets.

28. (PREVIOUSLY PRESENTED) The router of claim 27, wherein the means for reordering is configured for reordering, in each queuing means, the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface.

29. (ORIGINAL) The router of claim 27, wherein the means for reordering is configured for, in each queuing means:

establishing a plurality of queues having respective identified priorities;

storing each data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each data packet; and

selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy.

30. (ORIGINAL) The router of claim 27, wherein:

the means for establishing is configured for establishing, on each of a plurality of the outbound interfaces, a corresponding plurality of the secure connections with a corresponding

plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the generating means;

the controlling means is configured for controlling the supply of data packets, for each outbound interface, based on the assigning means assigning, for each secure connection for each outbound interface, a corresponding one of the queuing means;

the router further comprises routing means for selecting one of the outbound interfaces for each said data packet, the generating means configured for outputting each encrypted packet to the corresponding selected one of the outbound interfaces selected by the routing means.

31. (ORIGINAL) The router of claim 27, wherein the generating means is configured for outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol.

32. (CANCELED).

33. (CANCELED).

34. (ORIGINAL) The router of claim 27, wherein the reordering means is configured for obtaining the corresponding assigned maximum output bandwidth from a configuration register.

35. (ORIGINAL) The router of claim 27, wherein the reordering means further includes means for negotiating, for at least one queuing means, the corresponding assigned maximum output bandwidth with the corresponding destination.

36. (PREVIOUSLY PRESENTED) The method of claim 1, wherein each secure connection is a corresponding encrypted tunnel.

37. (PREVIOUSLY PRESENTED) The router of claim 10, wherein each secure connection is a corresponding encrypted tunnel.

38. (PREVIOUSLY PRESENTED) The medium of claim 18, wherein each secure connection is a corresponding encrypted tunnel.

39. (PREVIOUSLY PRESENTED) The router of claim 27, wherein each secure connection is a corresponding encrypted tunnel.

40. (NEW) The method of claim 1, wherein:

the router includes the outbound interface, the cryptographic module, and each of the queueing modules;

the establishing of the IP-based secure connections, the controlling supply of data packets, and the second outputting of the encrypted packets to the outbound interface each executed in the router.